

## REMARKS

### **I. General**

#### **A. Issues**

Claims 1-36 were pending the Application and according to the Office Action dated February 4, 2009 (hereinafter *Office Action*), each claim stands rejected. The drawings are listed as objected to. Claims 1, 12, and 19 stand rejected under 35 U.S.C. § 101 as being directed to non-statutory matter. Claims 1-36 stand rejected under 35 U.S.C. § 102(c), as being anticipated by Soong United States Patent No. 6,941,271 (hereinafter *Soong*).

#### **B. Claim Amendments**

Claims 1, 4, 5, 12, 13, 14, 16, 20-24, 28, 29, 34, 35, and 36 are amended herein. Claim 6 is canceled without prejudice, and new claims 37-40 are added. Support for each of the newly added limitations can be found in the specification, *see e.g.*, Figures 3-5 and their corresponding description in paragraphs [0027]-[0034] of the originally filed specification; and thus, no new matter has been added.

### **II. Examiner Interview Summary**

On April 28, 2009, a telephone discussion was held between the Examiner, Sheetal Rangrej, and Applicant's representatives Jody Bishop and Lisa Joni Collins. Applicant would like to express appreciation to the Examiner for her time and consideration in discussing this application. Applicant respectfully submits this summary of the substance of the discussion in accordance with M.P.E.P. §713.04.

First, Applicant's representatives discussed the disclosure of the *Soong* reference. Applicant's representatives noted that *Soong* generally discloses a traditional patient-centric method used for managing access to centrally-stored medical records in a web accessible database. In Soong's traditional system, patient medical records are stored in a centralized

database (*Soong* at col. 5, lns. 4-6) which allows a patient to create a password granting to access those files. *Soong* at col. 6, lns. 50-53. Once the patient is given a password, the patient can distribute the password to other individuals, such as physicians, who can use that password to log into the *Soong*'s system and access the records. *Soong* at col. 6, lns. 50-53. For example, if a patient wants his podiatrist, cardiologist, and physiatrist to have access to his medical records, the patient gives each of his doctors the password. See *Soong* at col. 6, lns. 50-53.

Once a doctor has a patient's password, when accessing the patient's medical records, the doctor must log into *Soong*'s system and input the patient's password. *Soong* at col. 6, lns. 19-25. Once the password is entered, the *Soong*'s system verifies the password and allows access if the password is valid. *Soong* at col. 6, lns. 28-32.

Thus, the burden is placed on the individual physicians to maintain and input the various passwords provided the physicians by their patients. This typically leads to considerable overhead for the physicians because each physician must maintain a long list of passwords due to the multitude of patients providing individual passwords.

Applicant's representatives further noted that certain embodiments of the present invention provide an intermediary key organization system which aids in managing the various patient-defined access keys to facilitate access by the medical service providers to the patient's medical records. Applicant's representatives noted at least the following characteristics of certain embodiments of the present invention that are not taught by *Soong*:

First, in certain embodiments of the present invention, the key organization system associates an access key with a corresponding medical service provider to whom the access key is granted by a patient. Thus, for instance, the key organization system stores an association defining one or more medical service providers to whom the patient has granted the corresponding access key. The access key itself need not be provided to the medical service providers themselves. Instead, when the medical service providers access the key organization system (e.g., via a login), the associated access keys that have been granted to the providers can

be identified by the key organization system, and the associated keys may then be used for managing/controlling access by the providers to the medical records. *Soong* does not associate the passwords with any medical service provider to whom the corresponding access rights are granted. Instead, *Soong* associates a password with corresponding access rights, and then the site computer grants those access rights to any user who inputs the password.

Second, in certain embodiments of the present invention, the key organization system retrieves and uses the access keys for controlling access by a medical service provider to the medical records without requiring the medical service provider to maintain and input the access keys. Thus, whereas *Soong* requires a provider to input a password to the site computer in order to access the medical records of a particular patient who supplied the password to the provider, in certain embodiments of the present invention, the key organization system does not put the burden of maintaining and inputting to the key organization system different access keys for different patients in order to gain the patient-defined level of access to the patient medical records.

Applicant proposed submitting claim amendments to more specifically recite, in certain claims, certain aspects of the key organization system disclosed by embodiments of the present invention, such as those aspects discussed above.

In addition, the objections to the drawings raised in the Office Action were discussed, and Applicant's representatives noted that while the different label numbers 12, 14, and 16 are all used for referring to access keys, they refer to different access keys, such as corresponding access keys granted by the different patients 20, 22, and 24, respectively. The Examiner agreed that the objection to the drawings should be withdrawn.

### III. Objections to the Drawings

The drawings are listed as objected to as failing to comply with 37 CFR 1.84(p)(4) in the current Office Action. *Office Action* at 2. The *Office Action* states the objection is based on

"reference characters '12', '14', and '16' all being used to designate 'access keys'; reference characters '20', '22', and '24' all being used to designate 'medical records.'" *Office Action* at 2. As discussed above, during the Examiner Interview, the objections to the drawings were discussed, and it was agreed that the objection should be withdrawn without any new or amended drawings being required.

#### IV. 35 U.S.C. § 101 rejections

Claims 1, 12, and 19 are listed as rejected under 35 U.S.C. § 101 as being directed to non-statutory matter. *Office Action* at 3-4. While Applicant believes the originally filed claims are directed at statutory subject matter, Applicant has amended the claims herein to expedite prosecution.

According to *In re Bilski*, a claim is surely patent eligible under § 101 if it satisfies the so-called machine-or-transformation test by either being tied to a particular machine or apparatus or by transforming a particular article into a different state or thing. *In re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008). As amended herein, each of the method claims more clearly recite a machine, and thus are believed to clearly satisfy at least the machine prong of the machine-or-transformation test. As such, Applicant respectfully requests the rejection of record be withdrawn.

#### V. 35 U.S.C. § 102 rejections (*Soong*)

Claims 1-36 stand rejected under 35 U.S.C. § 102(e) as being anticipated by *Soong*. *Office Action* at 5. However, it is well settled that to anticipate a claim, a reference must teach every element of the claim, see M.P.E.P. § 2131. Moreover, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, "[t]he elements must be arranged as required by the claim," see M.P.E.P. § 2131, citing *In re Bond*, 15 U.S.P.Q.2d 1566 (Fed. Cir. 1990). Furthermore, in order for a reference to be anticipatory under 35 U.S.C. § 102 with respect to a claim, "[t]he identical invention must be shown in as complete detail as is contained in the . . . claim," see M.P.E.P. § 2131, citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226,

1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989). Applicant respectfully asserts that the rejections do not satisfy these requirements, as detailed below.

**A. Receiving and Storing Access Keys**

**Independent claim 1** recites, in part, “receiving, by a key organization system operable on a computer processor, a first access key ...; receiving, by said key organization system, a second access key ...; storing the first and second access keys in a centralized key repository that is communicatively accessible by said key organization system” (emphasis added).

**Independent claim 12** recites “receiving, by the key organization system from a first patient using a client computer, a first access key ...; receiving, by the key organization system from a second patient using a second client computer, a second access key ...; storing, by said key organization system, the first and second access keys and said association in a centralized key repository” (emphasis added). **Independent claim 35** recites “receive, from a patient at a key organization system, a first access key ...; receive, from said patient at said key organization system, a second access key ...; store the first and second access keys in a centralized key repository” (emphasis added). **Independent claim 36** recites “a key organization system to: store a plurality of provider-associated access keys on a centralized key repository, wherein said plurality of provider-associated access keys comprise a first access key that grants a patient-defined level of access to the first set of medical records and a second access key that grants a patient-defined level of access to the second set of medical records” (emphasis added). As discussed below, *Soong* fails to teach at least the above-emphasized limitations of claims 1, 12, 35, and 36.

The *Office Action* likens *Soong*’s password to the claimed “access keys.” *Office Action* at 5. However, *Soong* does not teach a key organization system that receives and stores access keys. *Soong*’s distribution of passwords does not teach the limitation. Specifically, *Soong* teaches that the patient can provide the password to others. *Soong* at col. 6, lns. 50-54. However, in *Soong*, the distributed passwords are not taught as stored in any intermediary system (e.g. a key organization system). Rather, after the passwords are distributed in *Soong*, it becomes the responsibility of the individual recipients of such passwords to keep track of the passwords

and to input the passwords when accessing the medical records. *Soong* at col. 6, lns. 49-59. As such, *Soong* does not teach a key organization system receiving and storing access keys.

Therefore the rejection of claims 1, 12, 35, and 36 should be withdrawn for at least the above reasons.

#### B. Associating Access Keys

**Claim 1** recites “associating, by said key organization system, said first and second access keys with said medical service provider”. **Claim 12** recites “associating, by said key organization system, said first and second access keys to said medical service provider ... storing, by said key organization system, the first and second access keys and said association in a centralized key repository”. **Claim 28** recites “a first access key associated with a medical service provider that grants to said medical service provider a patient-defined level of access to the first set of medical records ... [and] a second access key associated with said medical service provider that grants to said medical service provider a patient-defined level of access to the second set of medical records”. **Claim 35** recites “a first access key associated with a first medical service provider that grants to said first medical service provider a first patient-defined level of access to a first set of medical records ... [and] a second access key associated with a second medical service provider that grants to said second medical service provider a second patient-defined level of access to said first set of medical records”. **Claim 36** recites “a plurality of provider-associated access keys . . .”. *Soong* fails to teach at least the above limitations, as discussed below.

*Soong*’s passwords are not associated with a medical provider. In *Soong*, the patient merely provides his password to whomever (e.g. family members, friends, health care professionals), and any of those individuals use that same patient password to access the medical records. *Soong* at col. 6, lns. 5-6, 50-54. Thus, while the password may define certain access rights that are presumed by the system as being granted to the individual inputting the password, the system does not associate the password with any medical service provider. For instance, the system makes no determination of whether a given password has been granted to a particular

medical service provider (or other user) who is requesting access to the medical records, but instead merely requires the requestor to input the password.

Therefore the rejection of claims 1, 12, 28, 35, and 36 should be withdrawn for at least the above reasons.

**C. Receiving and Associating Different Access Keys from the Same Patient with Different Providers**

Claim 34 recites “receive, at said key organization system, a first access key that grants to a first medical service provider a first patient-defined level of access to a first set of medical records of a corresponding patient; [and] receive, at said key organization system, a second access key that grants to a second medical service provider a second patient-defined level of access to said first set of medical records of said corresponding patient” (emphasis added). Claim 35 recites “receive, from a patient at a key organization system, a first access key associated with a first medical service provider that grants to said first medical service provider a first patient-defined level of access to a first set of medical records; [and] receive, from said patient at said key organization system, a second access key associated with a second medical service provider that grants to said second medical service provider a second patient-defined level of access to said first set of medical records” (emphasis added). *Soong* fails to teach the above limitations of claims 34 and 35.

Just as *Soong* does not teach a key organization system receiving or associating an access key with a particular provider as explained above, *Soong* does not teach a key organization system receiving or associating different access keys from the same patient which are associated with different providers. Therefore the rejection of claims 34 and 35 should be withdrawn for at least the above reasons.

**D. The Key Organization System Uses the Access Keys to Control Access**

Claim 19 recites “responsive to a request received from a medical service provider to access one of said sets of medical records, retrieving, by a key organization system, from said

centralized key repository a determined one of said access keys that is associated with said medical service provider and which corresponds to said requested set of medical records, and controlling, by said key organization system, access by said medical service provider to said requested set of medical records using the retrieved access key" (emphasis added). Claim 28 recites "wherein the key organization system is configured to, responsive to receipt of a request from the medical service provider to access one of said first and second set of medical records, retrieve a determined one of the first and second access keys from the centralized key repository and use the retrieved access key to control access by said medical service provider to said requested set of medical records" (emphasis added). Claim 34 recites "responsive to a request received from one of said first and second medical service providers to access said first set of medical records, retrieve from said centralized key repository a determined one of said access keys that is associated with said requesting medical service provider, and using the retrieved access key to grant to the requesting medical service provider the corresponding patient-defined level of access to said first set of medical records" (emphasis added). Claim 36 recites "responsive to a received request from a provider to access one of said first and second sets of medical records, retrieve from said centralized key repository a respective one of said first and second access keys that grants the requesting provider a patient-defined level of access to the requested one of said first and second sets of medical records; and use said retrieved access key to grant said requesting provider the corresponding patient-defined level of access to the requested one of said first and second sets of medical records" (emphasis added).

*Soong* does not teach the above limitations of claims 19, 28, 34, and 36. Rather than retrieving and using a key from a centralized key repository, *Soong* requires a requesting user (e.g., physician) to input a password that is used for controlling access to the medical records. Therefore, the rejection of claims 19, 28, 34, and 36 should be withdrawn for this further reason.

**E. Provider Accesses Medical Records without Inputting the Access Key**

Independent claim 12 recites "receiving, by said key organization system, a request from said medical service provider to access said first or second set of medical records and,



responsive to said request, controlling access to said requested set of medical records using said first or second access key, wherein input of said first or second access key from said medical service provider is not required by said key organization system" (emphasis added). Claim 35 recites "receive a request from said first medical service provider to access said first set of medical records; and retrieve, responsive to said request, said first access key from said centralized key repository to provide said first medical service provider with access to said first set of medical records wherein input of said first access key from said first medical service provider is not required by said key organization system" (emphasis added).

*Soong* does not allow a service provider to access medical records without first inputting a password. *Soong* at col. 6, lns. 20-25. Rather, *Soong* requires that the patient's password be entered by the individual person requesting the medical records before access to the records will be provided. *Soong* at col. 6, lns. 20-25. As such, *Soong* does not teach the above limitations of claims 12 and 35, and thus the rejection of these claims should be withdrawn for this further reason.

### Dependent Claims

Dependent claims 2-5, 7-11, 13-18, 20-27, 29-33, and newly- added claims 37-41 depend either directly or indirectly from independent claims 1, 12, 19, and 28 and thus inherit all of the limitations of their respective base claim. It is respectfully submitted that each of the dependent claims are allowable at least because of their dependence from their base claim for the reasons discussed above.

## VI. Conclusion

In view of the above, applicant believes the pending application is in condition for allowance.

Applicant believes that a fee of \$156.00 is due with this response and is being paid online by credit card. If any additional fees are due, please charge any fees required or credit any overpayment to Deposit Account 06-2380 under Order No. 66729/P032US/10614704 during the pendency of this Application pursuant to 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Dated: May 4, 2009

Respectfully submitted,

By 

Jody C. Bishop  
Registration No.: 44,034  
FULBRIGHT & JAWORSKI L.L.P.  
2200 Ross Avenue, Suite 2800  
Dallas, Texas 75201-2784  
(214) 855-8007  
(214) 855-8200 (Fax)  
Attorney for Applicant